STAPLES
Business Advantage

WHITE PAPER

K–12 Cybersecurity: How to Establish Best Practices at Your School

With the continued growth of technology use by students and staff alike, the need to protect data and users from cyberthreats has never been more critical. Here's a seven-point approach to identify and resolve network vulnerabilities.

Schools face a daunting challenge when it comes to cybersecurity.

The concerns are real: In a review of 159 school districts, an EdTech Strategies team found that 43 percent "make no attempt to secure communications with their websites, actively redirect website users to insecure connections or have configuration errors that break website security."

The potential exists for bad actors to take advantage of such vulnerabilities and introduce malware or use loopholes to gain access and manipulate systems or tamper with data.

"In sum, state and local education agency websites appear to be lagging behind other online sites in providing secure browsing protections to their users," noted the EdTech Strategies report, "Education Agency Website Security and Privacy Practices."

"Virtually all state and local education agency websites suffer from configuration errors and/or were found to have not implemented a significant number of website security best practices," the research discovered.

Equally worrisome, these vulnerabilities exist at a time when 70 percent of principals have plans to buy more laptops, tablets and other hardware products for their student users — creating increased avenues for cybercriminals. That's an uptick in planned purchases from 48 percent in 2017, according to research by MCH Strategic Data, "K–12 Principals' Assessment of Education: 2018 Edition."

Simultaneously, systems administrators in schools often struggle to keep up with tech-savvy students who push their access limits, perhaps to modify grades, violate the privacy of their classmates or simply to satisfy themselves that they can defeat security controls.

1/10

The number of educational organizations that suffered ransomware attacks during the last year

SOURCE: BitSight Technologies, "The Rising Face of Cyber Crime: Ransomware," September 2016

On the Offensive

Operating educational technology systems in this environment requires that school technology staffs have a strong understanding of cybersecurity and take proactive measures to defend their schools and districts against a variety of attacks.

Gone are the days when security can simply be a side responsibility of a school's IT manager. Larger districts now employ dedicated cybersecurity teams with responsibility for monitoring and managing security controls.

What follows are seven projects that will help the IT team bolster network security immediately and build the foundation for maintaining threat-resistant environments.

Project 1: Complete a Cybersecurity Assessment of Your Network

The goal of the cybersecurity assessment is to take a comprehensive look at the school's existing controls and identify any gaps that might require attention from technology administrators.

Schools and districts may approach this assessment in a number of ways. If the organization doesn't have skilled cybersecurity experts, it may choose to outsource this assessment to a qualified provider. On the other hand, it might find that using internal staff with appropriate qualifications is much more cost-effective.

Comprehensive assessments should follow a standard cybersecurity framework. Many organizations choose to adopt the Cybersecurity Framework published by the National Institute of Standards and Technology as their program baseline and then conduct an assessment against that framework. Others might choose to focus on specific areas of concern.

At a minimum, a school's cybersecurity assessment should consist of three important elements: conducting an account and user privileges review, running network vulnerability scans, and reviewing firewall rules.

Schools may choose to add other elements to the assessment based upon their specific needs and risk profile. For instance: What interdependencies are there among systems? How is data shared across systems? And what types of internal and external interfaces exist?

Project 2: Conduct Account and Privilege Reviews

One of the best places to start an assessment is with a review of the existing user accounts on the school's network. Unless the school recently performed a review, there's a high probability that accounts exist on the network that belong to faculty, staff and students who have left the organization (perhaps long ago).

This portion of the review is fairly straightforward. Begin with the list of user accounts and the list of current faculty, staff and students. Then simply compare the two lists, looking for any accounts that don't map to an authorized user. Once you have the list of discrepancies, walk through each of those to resolve them. You'll likely find that you have a significant number of unnecessary accounts you can remove.

To help manage this process across a school or district infrastructure, IT teams can use identity access management tools, which will scan the network looking for new accounts and report out their access privileges.

After ensuring that only authorized users have accounts on the network, the next step is to dig into specific permissions granted to each user. This will require some customization based upon the systems and applications used by your school, but the basic idea is to walk through each of those systems and ensure that users only have the access necessary to complete their jobs.

The customization of identify access management ties to risk. Prioritize systems and networks according to the impact that a breach, data loss or downtime will have — then tier the privilege reviews and the hurdles to access accordingly.

Watch out for cases of privilege creep, where people retain permissions associated with roles they no longer hold. This process will reveal accounts that require permission adjustments.

In addition to repeating account and privilege reviews on a periodic basis, IT teams should use the results to guide adjustments to whatever practices exist for creating and deprovisioning user accounts.

If reviews turn up a large number of accounts belonging to retired faculty, for example, look at the faculty retirement process and see if there's a good place to insert a step that ensures accounts are terminated upon the faculty member's last day of employment.

By regularly conducting these reviews, the school or district should see fewer and fewer unnecessary accounts turning up during subsequent reviews.

How Attackers Target K–12 Environments

Every sector has its unique security challenges. Education, for instance, tends to attract distributed denial of service (DDoS) attacks.

This and cybercriminals' focus on social engineering tactics, like phishing, make sense. As Verizon's "2018 Data Breach Investigations Report" points out: "Typically, there is more transparency in educational institutions regarding the disclosure of data such as the names, job roles and contact information of employees than exist in other verticals and this no doubt aids the attacker in those situations."

Here are a few data points about school threats gleaned from the report that can help focus security efforts:

72%

The percentage of incidents attributable to hacking

44%

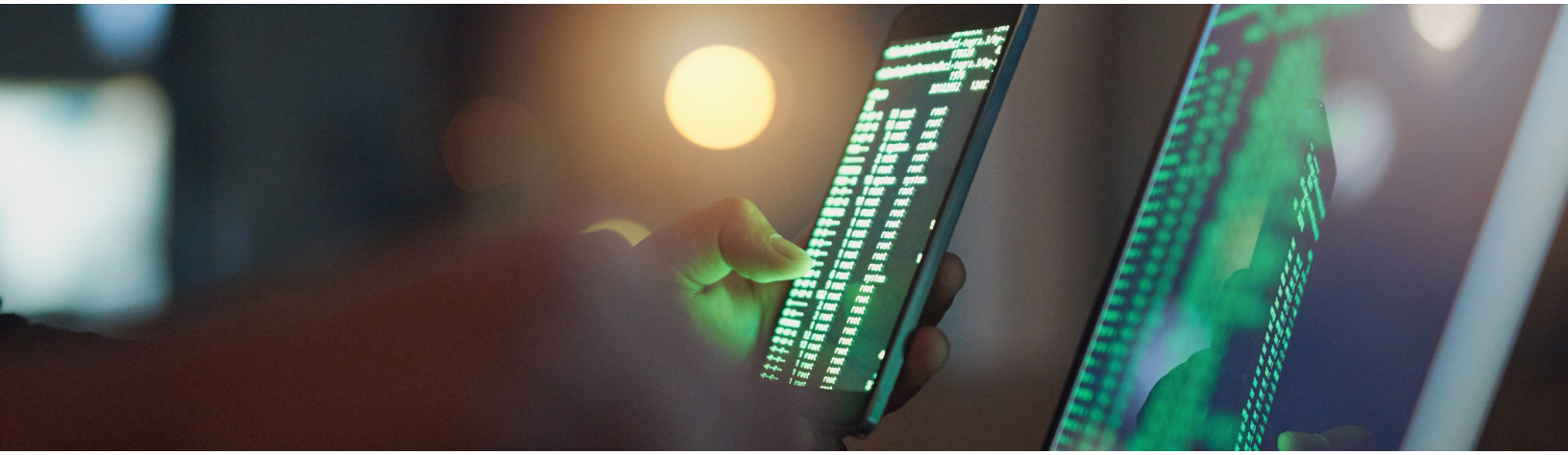
The percentage of non-DDoS attacks in which backdoor vulnerabilities or stolen credentials were used to gain access

41%

The percentage of breaches involving some form of social attack

16%

The percentage of insider incidents caused by user errors



Project 3: Implement Network Vulnerability Scanning

The modern network is a complex collection of servers, workstations, printers, internet of things (IoT) devices, mobile phones, tablets and almost anything else with a power button. School networks host everything from web applications for student records to vending machines that require connectivity to report inventory levels.

A single security issue on any of these devices can present an attacker with an opportunity to gain an initial foothold in the network and then leverage that access to further compromise the security of increasingly sensitive school systems. Network vulnerability scanning helps IT administrators keep an eye on the diverse residents of their networks and proactively identify and remediate security issues.

Vulnerability scanners, sold by many security systems makers, use software programs to search a district's network for connected devices and then probe those devices for thousands of known vulnerabilities.

For instance, a scanner will look for holes in services and ports, irregularities in data packets on the network, questionable web activities, and any paths available to reach exploitable programs or scripts. It then reports back these results, providing a prioritized list of issues rated by the severity of the vulnerability and laying out a road map for remediation.

Issues identified during these scans vary widely in type and severity. For example, a scan might reveal out-of-date systems that require operating system patches to bring them back to a secure state.

"Network vulnerability scanning helps IT administrators keep an eye on the diverse residents of their networks and proactively identify and remediate security issues."

The same scan might also detect that a web app contains an SQL injection flaw — in other words, structured query language code introduced surreptitiously by a cybercriminal to gain unrestricted access to an underlying database (with the hope that no one will spot the malicious code). It might also show that student workstations lack simple security controls that could allow the systems to become the entry point for attacks.

Regardless of size, every school and district should have a vulnerability scanning solution and run periodic scans of the entire network. It's critical to remember, however, that just running the scans doesn't improve security.

Vulnerability scanners are designed to point out issues that systems administrators must then act on to remediate. Then, sysadmins should rerun the scan to verify that they properly resolved the issues. Schools that follow this cyclic vulnerability identification and remediation process will find it dramatically improves the state of network security.

Project 4: Update and Maintain Firewall Rules

Firewalls are the workhorses of network security. They sit at the perimeter of the school network and moderate all access to internal resources by external systems. Firewalls prevent outside attackers from entering the network. They also sit in between network zones, serving a similar purpose.

For example, in an academic setting, a firewall might be used to prevent systems that are segmented onto a dedicated student network from accessing administrative servers, while allowing faculty systems to access those same servers.

Firewalls perform this function by enforcing a set of policy rules that describe the specific types of network activity that are permitted to pass through the firewall. It will block any activity not explicitly permitted by a rule. When the school introduces a new system that requires external access, network administrators must adjust the firewall policy rules to allow such access.

Firewall rule bases can quickly become complex and grow to the point where it can become difficult, if not impossible, for a single person to understand the entire firewall rule base. That creates a situation that's ripe for error, and it's not unusual to find that the firewalls at larger schools and districts contain hundreds of rules, dozens of which are either incorrect or no longer needed.

Just as schools should conduct periodic account reviews to ferret out unnecessary accounts and privileges, network administrators need to conduct firewall reviews to ensure that all of the rules in the firewall rule base continue to be correctly designed and necessary to meet current requirements. They should remove rules that don't pass muster to avoid allowing unintended access to the school network.

370+

The number of security incidents reported by schools since January 2016

SOURCE: EdTech Strategies, The K–12 Cyber Incident Map

197

The average number of days it takes for an organization to identify that a security breach occurred

SOURCE: Ponemon Institute, 2018 Cost of a Data Breach Study

How to Determine the Right Cybersecurity Budget

Most schools and districts operate on tight budgets.

In 2015, the year for which the most recent U.S. Census data are available, the funding for IT per student in 29 states was below what it had been in 2008, according to the Center on Budget and Policy Priorities.

However, due diligence requires that each school establish a cybersecurity program and provide it with the necessary staffing and funding to protect the confidentiality, integrity and availability of school information and critical systems.

For Projects and New Implementations

Security projects and the implementation of new technologies are major components of a cybersecurity program's budget. Staying ahead of the evolving threat facing schools and districts requires keeping up to date on modern security controls and implementing new tools as technology improves.

While most schools now have network firewalls in place to protect their networks, many do not have data loss prevention (DLP) or security information and event management (SIEM) systems that serve as two of the cornerstones of a modern cybersecurity program.

The gap analysis done after conducting a school's cybersecurity assessment will likely point out the need for both short-term and long-term projects. These projects will require one-time funding to design controls, acquire equipment and implement new technology.

To stay ahead of evolving threats, schools and districts must ensure their IT budgets let them keep security controls and tools up to date.

For Maintenance, Upgrades and Replacements

Once a school implements a robust cybersecurity program, the technology supporting that program requires ongoing funding to maintain it. This includes vendor support fees required to receive security updates and technical support, as well as funding to replace hardware as it ages.

Failure to invest in ongoing maintenance, upgrades and replacement will inevitably lead to the decay of a school's cybersecurity controls and expose it to risk.

For Staff

Technology is an important piece of the cybersecurity puzzle, but it's not the most crucial element. Sophisticated cybersecurity technology requires skilled staff to operate and maintain it. For example, a SIEM that provides a security alert is only useful if a technologist trained in incident response is able to receive and react to that alert.

School districts should ensure that they have at least one person on their technology team well-versed in cybersecurity technologies and practices. Ideally, cybersecurity responsibilities should be shared across a team of trained staff members to ensure redundancy and backup for emergency scenarios. But that might not be financially possible in smaller districts.

As schools and districts build out their budgets, creating a skilled cybersecurity team should be a significant long-term priority. At the same time, budgets should include professional development funds for cybersecurity staff members.

The constantly evolving nature of cybersecurity requires continuous training and skill development. Without this training, the skills of team members will atrophy and retaining skilled staff will become challenging.

Project 5: Protect Against Insider Threats

When school leaders think about cybersecurity risks, their minds naturally turn to far-off threats, such as remote cybercriminals, ransomware and viruses. These are all legitimate concerns. But schools also must not overlook the more insidious threat from within their own organizations.

Students, parents, faculty, staff and others with authorized access to systems might seek to exceed their authorized access privileges and jeopardize the security of school systems and sensitive information. According to Verizon's "2018 Data Breach Investigations Report," 19 percent of security breaches are attributable to internal actors.

As schools develop their cybersecurity programs, they need to keep the insider threat front of mind and implement controls designed to counter it. As already mentioned, appropriate access management is critical. Additionally, endpoint security tools that monitor user activities and report anomalies can tip IT to actions that suggest possible threats.

It's particularly important because sometimes these breaches are not malicious but accidental. That means IT teams also need to provide guidance and training about security best practices and about reporting anything suspicious, such as phishing attack attempts or out-of-the-norm behavior. That won't stop a malicious actor, but it will help lessen the potential for unknowing users creating additional vulnerabilities.

42%

The percentage of 159 school districts in a cybersecurity review that offer partial security to all of their users. "In every one of these cases, however, each of these school district websites is still in need of improvement and reporting potentially significant vulnerabilities."

SOURCE: EdTech Strategies, "Education Agency Website Security and Privacy Practices," January 2018

Cybersecurity Profile

Business Objectives

Threat Environment

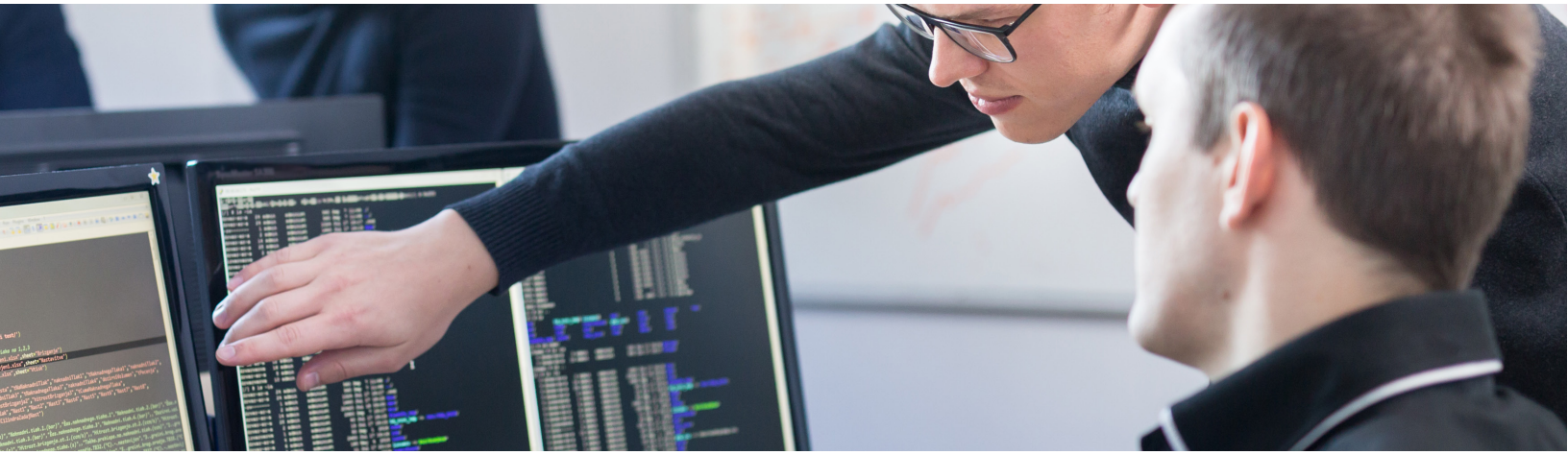
Requirements and Controls

What Makes Up Your Cybersecurity Profile?

The National Institute of Standards and Technology (NIST) built its widely used framework on five core functions: identify, protect, detect, respond and recover. For each function, NIST provides detailed guidance and resources for establishing cybersecurity practices against desired outcomes.

As part of the development of a custom framework using the NIST approach, a school or district would create a cybersecurity profile that aligns its unique mission, environment and risk tolerance with the desired cybersecurity outcomes for the five core elements of the framework.

SOURCE: NIST, "Cybersecurity Framework," April 2018



Project 6: Implement Data Loss Prevention

One of the most significant security challenges facing schools is protecting the confidentiality of sensitive information. The Family Educational Rights and Privacy Act (FERPA) places the burden of maintaining confidentiality squarely on the shoulders of schools nationwide, while state and local privacy and data breach notification laws also impose obligations on schools and districts.

Data loss prevention (DLP) systems provide technology that helps schools safeguard their most sensitive information and prevent insiders from maliciously or accidentally removing it from secure network locations. DLP technology works by monitoring systems and networks for signs of sensitive information.

It does so using two primary techniques: signature detection and watermarking.

Signature detection watches data leaving the network for signs that it contains sensitive information. For example, a Social Security number appearing in a student record might trigger a signature detection rule, as would a credit card number embedded in an activity fee payment receipt.

Signature detection works well at detecting these predictable forms of sensitive information, but it is less effective at identifying sensitive information that doesn't follow a structured pattern. That's where watermarking comes in.

In a watermarking approach, administrators embed a special signature in files containing sensitive information, which identifies them as sensitive.

When a DLP system detects an attempt to remove sensitive information from the school's network, it triggers an automated response that varies depending upon the method used to remove the information.

For instance, the DLP system might place a suspect email message in a quarantine queue for administrator review. It might block an attempt to upload a student record file to an insecure location or prevent a user from copying watermarked files to a USB drive.

The actions the system takes are based on default and custom policies enacted by the IT team. Typically, the baseline policies will look for personally identifiable information, protected health information, credit card numbers and Social Security numbers.

But in a school environment, the IT and administrative staff will want to collaborate and define what is deemed "sensitive information" — things like test scores and grades, for instance.

DLP systems can help schools safeguard their most sensitive information and prevent insiders from maliciously or accidentally removing it from secure network locations.

Project 7: Establish a Data Reporting and Analytics Review Process

Security technologies generate massive amounts of information. They create log entries each time an individual is granted or denied access to resources, a firewall allows or blocks a network connection, a DLP system detects sensitive information theft, and more. The end result is millions of records generated each day.

Those records contain crucial information that may help administrators reconfigure the school's security systems to defend against emerging threats, but that information is often difficult to uncover. Security administrators find themselves facing a challenge equivalent to finding a needle in a haystack. It's simply not feasible to manually review millions of log entries each day.

According to the SANS Technology Institute, there are six log reports that are most critical in helping spot trouble as well as resolving it once disaster strikes:

1. **Authentication and authorization reports**
2. **Systems and data change reports**
3. **Network activity reports**
4. **Resource access reports**
5. **Malware activity reports**
6. **Failure and critical error reports**

Security information and event management (SIEM) systems provide an automated approach to managing the tedious work of extrapolating log data. These specialized systems receive and aggregate entries from a wide variety of security products and then automatically analyze them, looking for significant activity that requires either an automated response or administrator review. And they become smarter over time based on the behaviors of the users within the environment they monitor.

A SIEM system looks for the activities and behaviors that stand out or might signal malicious activity. The power of SIEM comes from the technology's ability to correlate information from multiple sources.

A SIEM might notice repeated failed attempts to connect to the school's virtual private network using the principal's account followed by a successful attempt by the principal to download massive quantities of information. Either one of those activities in isolation might be shrugged off, but together they indicate a potential security incident.

The power of aggregation and correlation makes a SIEM a crucial tool in the arsenal of any school technology team. But just as with other security tools, a SIEM depends on the rules created for it. The IT team will need to identify the logs that make sense for the school or district, and then set the reporting based on risk of data exposure. And again, these cannot be "set it and forget it" rules. The IT team should review them quarterly.

By diligently undertaking these seven projects and implementing the appropriate technology tools, a school's or district's IT team can reduce the exposure of the network to threats and improve its preparedness to handle an incident when it inevitably happens.